Ukraine suffered more data-wiping malware than anywhere, ever

Celestino Arce/Getty Images

reader comments

25 with

Share this story

Amidst the tragic toll of Russia's brutal and catastrophic invasion of Ukraine, the effects of the Kremlin's long-running campaign of destructive cyberattacks against its neighbor have often—rightfully—been treated as an afterthought. But after a year of war, it's becoming clear that the cyberwar Ukraine has endured for the past year represents, by some measures, the most active digital conflict in history. Nowhere on the planet has ever been targeted with more specimens of data-destroying code in a single year.

Ahead of the one-year anniversary of Russia's invasion, cybersecurity researchers at Slovakian cybersecurity firm ESET, network security firm Fortinet, and Google-owned incident-response firm Mandiant have all independently found that in 2022, Ukraine saw far more specimens of "wiper" malware than in any previous year of Russia's long-running cyberwar targeting Ukraine—or, for that matter, any other year, anywhere. That doesn't necessarily mean Ukraine has been harder hit by Russian cyberattacks than in past years; in 2017 Russia's military intelligence hackers known as Sandworm

released the massively destructive NotPetya worm. But the growing volume of destructive code hints at a new kind of cyberwar that has accompanied Russia's physical invasion of Ukraine, with a pace and diversity of cyberattacks that's unprecedented.

"In terms of the sheer number of distinct wiper malware samples," says ESET senior malware researcher Anton Cherepanov, "this is the most intense use of wipers in all computer history."

Advertisement

Researchers say they're seeing Russia's state-sponsored hackers throw an unprecedented variety of data-destroying malware at Ukraine in a kind of Cambrian Explosion of wipers. They've found wiper malware samples there that target not just Windows machines, but Linux devices and even less common operating systems like Solaris and FreeBSD. They've seen specimens written in a broad array of different programming languages, and with different techniques to destroy target machines' code, from corrupting the partition tables used to organize databases to repurposing Microsoft's SDelete command line tool, to overwriting files wholesale with junk data.

In total, Fortinet counted 16 different "families" of wiper malware in Ukraine over the past 12 months, compared to just one or two in previous years, even at the height of Russia's cyberwar prior to its full-scale invasion. "We're not talking about, like, doubling or tripling," says Derek Manky, the head of Fortinet's threat intelligence team. "It's an explosion, another order of magnitude." That variety, researchers say, may be a sign of the sheer number of malware developers whom Russia has assigned to target Ukraine, or of Russia's efforts to build new variants that can stay ahead of Ukraine's detection tools, particularly as Ukraine has hardened its

cybersecurity defenses.

Fortinet has also found that the growing volume of wiper malware specimens hitting Ukraine may in fact be creating a more global proliferation problem. As those malware samples have shown up on the malware repository VirusTotal or even the open source code repository Github, Fortinet researchers say its network security tools have detected other hackers reusing those wipers against targets in 25 countries around the world. “Once that payload is developed, anyone can pick it up and use it,” Manky says.

https://arstechnica.com/?p=1919531